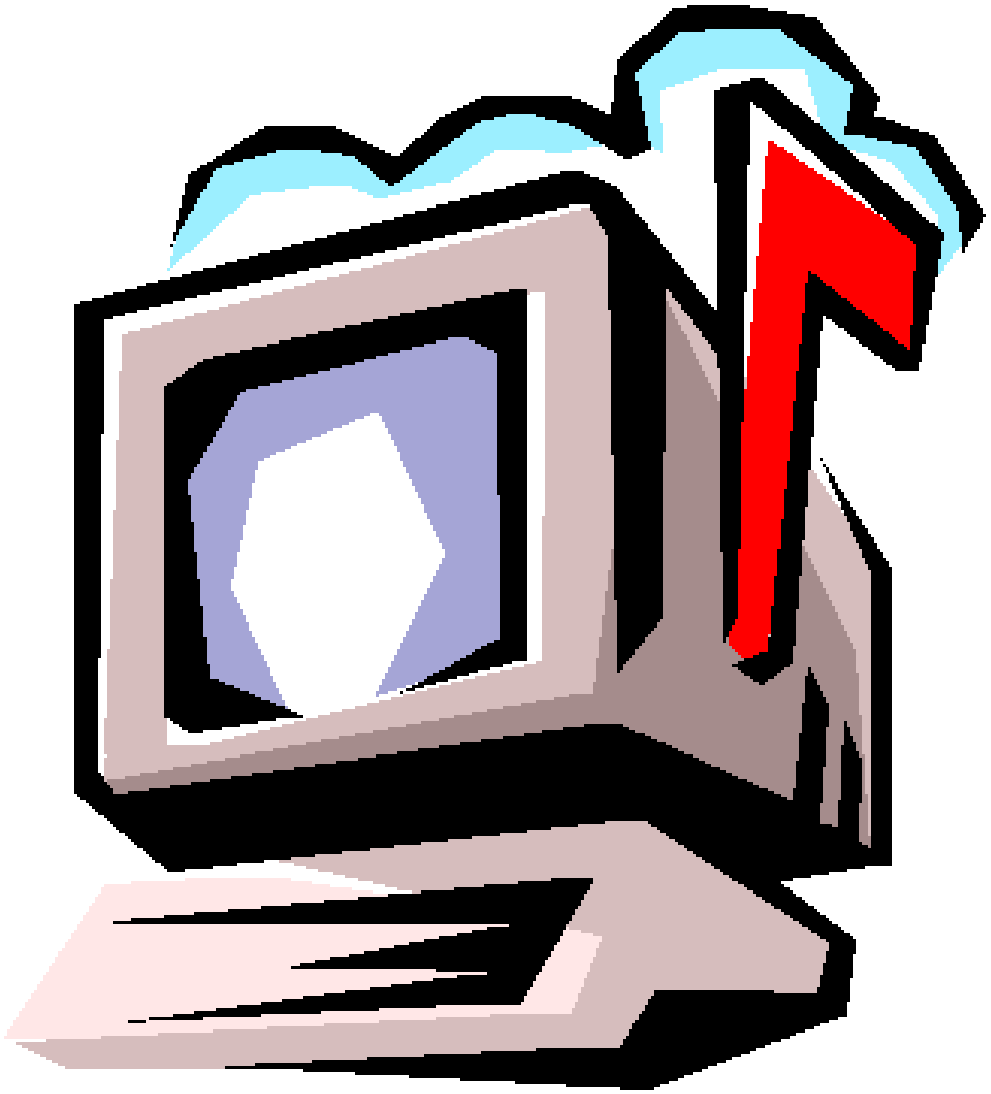


Why Encrypt Internet Email?

- HIPAA law requires covered entities to ensure integrity and confidentiality of health information
- HIPAA privacy rule sets strict limits on the disclosure of protected health information:
  - these can not be met if access is not controlled
  - Internet email can be intercepted and protected health information inappropriately disclosed

HIPAA Technical Requirements

- Integrity - ensure validity of information
- Authentication - message received matches message sent
- One of the following:
  - Access Controls so message can not be intercepted
  - Encryption

Encryption

The safest & most effective way to transmit information. It provides:

- Confidentiality
- Integrity - Message Authentication Code
- Authenticity - Digital Signature

How Encryption Works

- Transforms original into cipher text - leaves a string of seemingly random characters.
- Reverse process is decryption
- Has 2 basic elements:

  Algorithm - mathematical formula applied a number of times in different combinations.

  Key - a secret value related to the algorithm that controls substitutions and transpositions.

Methods/Category

Public and Private Key

- Private Key:

  A single key. The same key is used to encrypt & decrypt. The key is shared by both originator and the receiver.

  DES (Data Encryption Standard) is a private key system.

- Public Key:

  A two key system - public & private key.

  Private key is known only to the originator.

  Public key is shared.

  The two keys are mathematically related.

  RSA is best known public key system.

Private Key
Data Encryption Standard (DES)

- National standard adopted in 1977 as official method of protecting unclassified data in government computer systems.

- Private key cipher

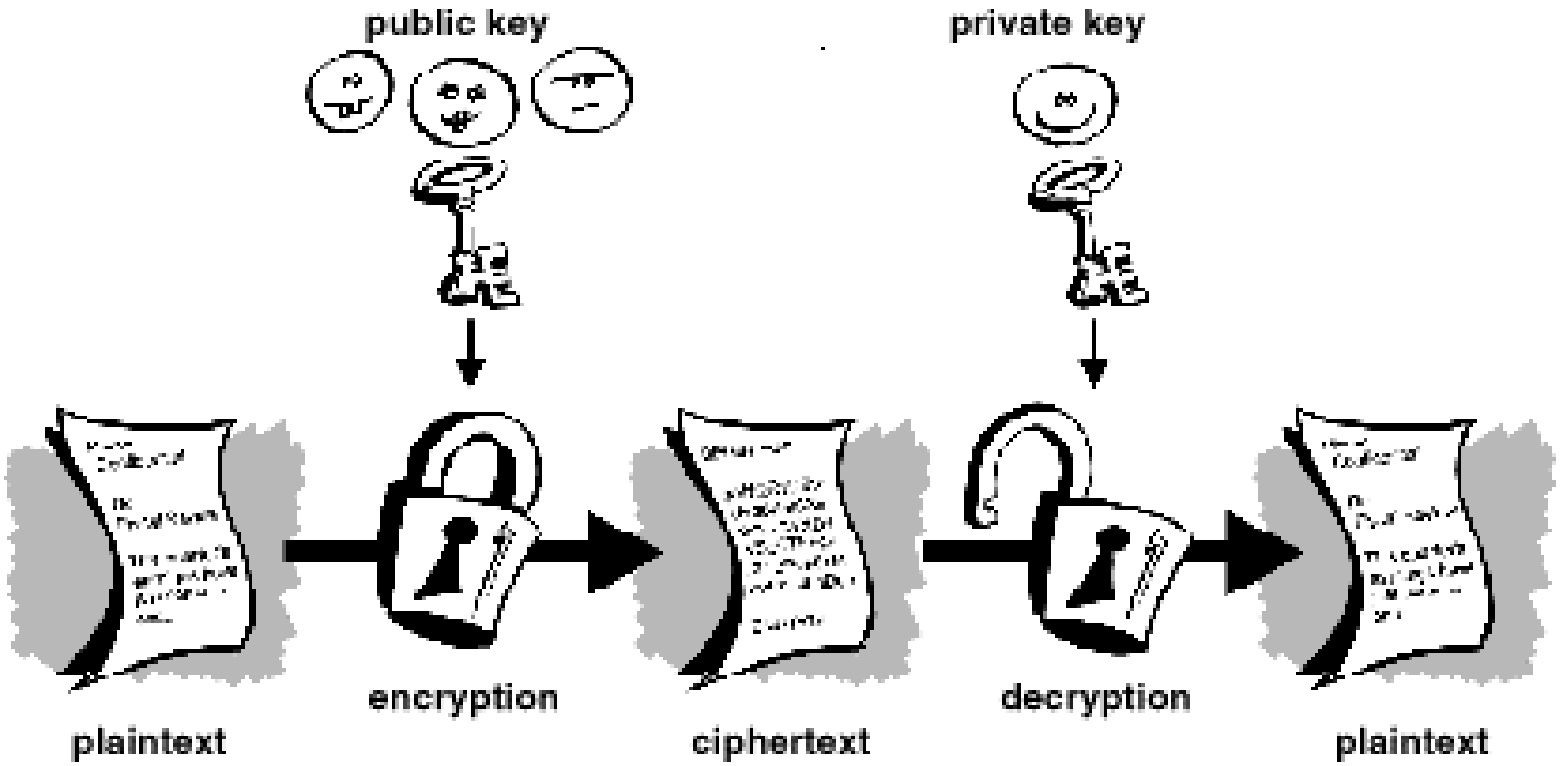
- Widespread use throughout industry

  Backbone of financial encryption between individuals, financial institutions, ATMs and POS terminals.

- Embedded in many commercial system products

Public Key
RSA (named for is developers)

- Uses extremely large numbers
- Each group of users has both a public key and a private key
- Public keys may be listed in e-mail directories
- Facilitates wider use of cryptography via larger user base
- In fairly widespread use outside of U.S. (algorithm published before patented.


public key
private key
encryption
decryption
plaintext
ciphertext
plaintext

SMIME

- Digital Signatures:
  - Verifies message origin and sender identity
  - Sender's key signs message, recipient's key validates
  - The digital signature is unique for every transaction

- Message Authentication
  - Insures message is not altered or a repeat
  - Appends an authentication code to the original message
  - Upon receipt the authentication code is independently calculated and compared to the incoming code

Key Management & Distribution

Security of cryptographic data depends on protecting the keys:

- Secure generation, distribution, storage, and discontinuation of keys.
- Protect keys from disclosure and substitution.
- Some networks automatically generate, transmit, and discontinue old keys.
- Initial keys in private systems still manually delivered in most cases.
- Must ensure that correct public keys are correctly identified by all users.
- Standards for key management have been developed by the government, ISO, ANSI, and American Banking Association.

- Evolving DHFS Secure E-Mail Policy for protecting identifiable health information
- Talk with email administrator - SMIME capability in email program.
- Talk with business partner(s) - SMIME capability in their email.
- Get digital key(s) - certificate authority.
- Test email with business partner(s).